

Math 104A, Number Theory, Fall 2002.
Summary of Lecture 16.

We mention here an observation which came up last time.

$$ac \equiv 0 \pmod{m} \quad \Leftrightarrow \quad a \equiv 0 \pmod{m}$$

The converse “ \Rightarrow ” is false in general, although it is true if $(m, c) = 1$. However,

$$ac \equiv 0 \pmod{m} \quad \Leftrightarrow \quad a \equiv 0 \pmod{\frac{m}{(m, c)}}.$$

Also, someone asked last time what we can say about the number of solutions to a polynomial congruence. We will see Lagrange’s theorem which says that the number of solutions to $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \equiv 0 \pmod{p}$ is at most n if p is prime.

Example. This is a simple example showing how you can solve a polynomial congruence by splitting the modulus into its prime factorization. Solve $x^2 \equiv 1 \pmod{6}$. To do this we notice that $6 = 2 \cdot 3$. We find that the equation $x^2 \equiv 1 \pmod{2}$ has the single solution $x \equiv 1 \pmod{2}$ and the equation $x^2 \equiv 1 \pmod{3}$ has two solutions $x \equiv 1 \pmod{3}$ and $x \equiv 2 \pmod{3}$. Now using the Chinese Remainder Theorem, we can write down the solution to

$$\begin{cases} x \equiv b_1 \pmod{2} \\ x \equiv b_2 \pmod{3} \end{cases}$$

and it is given by

$$x \equiv 3b_1 + 4b_2 \pmod{6}.$$

Plugging in $b_1 = 1$ and $b_2 = 1$ or 2 , we get the two solutions $x \equiv 7 \equiv 1$ and $x \equiv 11 \equiv 5 \pmod{6}$.

Lemma.

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0, \quad f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1,$$

we have

$$f(x_0 + p^k t) \equiv f(x_0) + p^k t f'(x_0) \pmod{p^{k+1}}.$$

To prove this, we use the binomial theorem to see that

$$f(x + y) = f(x) + y f'(x) + y^2 g(x, y)$$

where g is a polynomial of the two variables x and y . Indeed,

$$(x + y)^n = x^n + n x^{n-1} y + y^2 \left(\binom{n}{n-2} x^{n-2} + \dots + \binom{n}{0} y^{n-1} \right).$$

Example. Solve $x^2 + x + 3 \equiv 0 \pmod{45}$.

Solution. We note that $45 = 3^2 \cdot 5$. Modulo 3, we check that there are two solutions $x \equiv 0 \pmod{3}$ and $x \equiv 2 \pmod{3}$. Now for the solution modulo 9. The derivative of $f = x^2 + x + 3$ is $f' = 2x + 1$. We have

x	f'	f
0	1	3
2	5	9

Since $3 \nmid 1$ and $3 \nmid 5$ we get two solutions to $f(x) \equiv 0 \pmod{9}$, one of the form $x = 0 + 3t$ and the other of the form $x = 2 + 3t$. (The values of t in the two cases may of course be different!) To find t in the first case we solve

$$3 + 3t \equiv 0 \pmod{9} \Rightarrow 1 + t \equiv 0 \pmod{3} \Rightarrow t \equiv 2 \pmod{3}.$$

The value of x is thus $x \equiv 2 \cdot 2 \equiv 6 \pmod{9}$. In the second case we see directly that $f(2) \equiv 0 \pmod{9}$ and so the solution is $x \equiv 2 \pmod{9}$.

Now we solve $f(x) \equiv 0 \pmod{5}$ by trying all values of x modulo 5 we find two solutions $x \equiv 1 \pmod{5}$ and $x \equiv 3 \pmod{5}$.

Putting this together, we use the Chinese remainder theorem to solve

$$\begin{cases} x \equiv b_1 \pmod{9} \\ x \equiv b_2 \pmod{5}. \end{cases}$$

Since $1 = 5 \cdot 2 - 9$, the inverse of 5 modulo 9 is 2, and the inverse of 9 modulo 5 is 4. The solution is then

$$x \equiv 10b_1 + 36b_2 \pmod{45}.$$

Plugging in $b_1 = 2$ or 6 and $b_2 = 1$ or 3 gives the four solutions modulo 45,

$$x \equiv 56 \equiv 11, \quad x \equiv 128 \equiv 38 \equiv -7, \quad x \equiv 96 \equiv 6, \quad x \equiv 168 \equiv 33 \equiv -12.$$

We proved Theorem 3.4.6